# آليات التصدي للجريمة الرقمية في التشريع الجزائري

# Mechanisms to fight digital crime in Algerian legislation

د. درار عبد الهادي
جامعة أبو بكر بلقايد – تلمسان، (جمهورية الجزائر)

# آليات التصدي للجريمة الرقمية في التشريع الجزائري

***Mechanisms to fight digital crime in Algerian legislation***

**د. درار عبد الهادي**
**جامعة أبو بكر بلقايد – تلمسان، (الجزائر)**
**derrarm@hotmail.fr**

**ملخص:**

إن التطور الحاصل في مجال تكنولوجيا الإعلام والاتصال، وظهور الشبكة العنكبوتية (إنترنت) بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام؛ لأنه بقدر ما أحدث من آثار إيجابية وغَيَر نمط حياة المجتمعات وذهب بها إلى التطور والرقي في جميع المجالات، ولا سيما المعاملات الإلكترونية. بقدر ما كان له أثر سلبي على حياة الناس ومصالحهم ومصالح الدول، هذا كله تجلى في تطوير الإنترنت ووسائلها المعلوماتية لتكون عالماً من عوالم الجريمة. وهكذا ظهرت إلى الوجود الجرائم الإلكترونية بشتى أنواعها. لذلك سوف نخوض في التعرف على معنى هذه الجريمة المعلوماتية، وكيف تم التعامل معها من أجل مواجهتها.

**الكلمات المفتاحية:** القوانين الوطنية؛ المواجهة، المجرم الإلكتروني، القانون الدولي، الإتفاقيات الدولية، الأنترنت

**Abstract:**

The development in the field of information and communication technology and the emergence of the Internet with all its progress and services did not pass safely to the world because the extent that it has brought *positive* effects and changed the lifestyle of societies, and has advanced and developed all fields, especially electronic transactions, it has a negative impact on people's lives, their interests, and the interests of nations. All of this is manifested in the development of the Internet and its information means to be a world of crime. Thus, cybercrimes of all kinds appeared. Therefore, we will delve into the meaning of this cybercrime and how it was dealt with in order to confront it.

**Keywords:** national laws, confrontation, cybercriminal, international law, international agreements, Internet

**مقدمة:**

تواجه رقعة العلوم الجنائية اليوم أحدث وأخطر صور الجريمة التي انتشرت نتيجة المزاوجة بين تقنيات الإعلام الآلي وتكنولوجيا الاتصالات أو ما يعرف بثورة تكنولوجيا المعلومات وهي الجريمة المعلوماتية، الأمر الذي فرض على الدول ضرورة التدخل والتصدي لهذه الجرائم المستحدثة وكبح مخاطرها سواء على الأموال أو الأشخاص التي لم تعد منحصرة في إقليم الدولة الواحدة، وإنما تعداها ليصبح الأمر ذو شأن دولي، ما جعل الدول– ومنها الجزائر– تضع نصوصاً وتشريعات تواجه بها الإجرام، ولكن في غالبيتها تصطدم بفكرة تنازع الاختصاص القضائي إما على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي أو على أساس مبدأ الاختصاص العيني، الأمر الذي يفرض أن يكون هناك تعاوناً دولياً يتفق مع طبيعة الإجرام السيبراني الذي يتميز بطابع خاص يقتضي أن تكون هناك ردود فهل سريعة؛ لأن هذا التنسيق الفعال والعاجل يساعد على الحد من الأضرار الناجمة عن هذه الجرائم المعلوماتية وكذلك تجنب المجرم المعلوماتي الافلات من العقاب.

من خلال ما سبق تصاغ الإشكالية التالية: مدى كفاية النصوص التشريعية الجزائرية للتصدي للجريمة المعلوماتية؟ وهل تم حصرها ومجابهتها في إطار ما يعرف بالاتفاق أو التعاون الدولي؟

وللإجابة على هذه الإشكالية تم تقسيم الورقة البحثية إلى محورين رئيسيين: العنوان الرئيسي الأول: الإطار المفاهيمي للجريمة المعلوماتية، العنوان الرئيسي الثاني: ثبات النص الجزائري وتكامله مع الاتفاق الدولي لمواجهة الجريمة المعلوماتية.

## المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية

تتعدد أشكال السلوك السلبي وتتطور وتتخذ أشكالاً لا حصر لها تبعاً لما يتوفر بين يدي الإنسان من وسائل لإيقاع الفعل وتحقيق نتائجه في الواقع العملي.

وانطلاقاً من ذلك فقد ظهرت للوجود سلوكيات سلبية خطيرة تبعاً لظهور تقنية نظم المعلومات والاتصالات التي وضعت بين يدي البعض الفاسد وسائل وطرق حديثة لإيقاع جرائمهم بسهولة وخفة، فكان أن أحدثت هذه السلوكيات المستحدثة ثورة هائلة في النظرية العامة للجريمة على اختلاف مستوياتها[1].

[1] جلال محمد الزغبي، وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الأردن 2010، (ص 21).

وتُعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية التي تختلف كثيرا عن الجريمة التقليدية في طبيعتها وأنواعها وأدواتها، وحتى في خصوصية وتمييز مرتكبيها. وهذا ما سنعرج عليه من خلال هذا المحور.

## المطلب الأول: تعريف الجريمة الالكترونية

قبل الخوض في إعطاء تعاريف الجريمة الالكترونية لابد من الإشارة إلى المصطلحات المتعلقة بهذه الجريمة والتي نذكر منها:

1. **الحاسب الآلي**: هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصه لمعالجة وإدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي: استقبال البيانات المدخلة (الحصول على حقائق مجردة)، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المداخلات)، وإظهار المعلومات المخرجة (الحصول على نتائج)[1].

كما يُعرف بأنه: "أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو ارسالها أو استقبالها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له".[2]

ومن بين التعريفات التي أجمع عليها الفقه حول تعريف الحاسب الآلي: "مجموعة من الأجزاء المتداخلة المادية والمعنوية، وبتكامل هذه الأجهزة يقوم الجهاز باستقبال البيانات ومعالجتها من خلال مجموعة من العمليات الحسابية بسرعة عالية وتسلسل منطقي تظهر بعدها النتائج المطلوبة، ويمكن تخزينها والاستفادة منها مرات عديدة"[3]

2. **المعلومات**: وهي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات، بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.[4]

3. **كلمة إلكتروني**: يقصد بها تقنية استعمال وسائل كهربائية أو كهرومغناطيسية أو بصرية أو أي شكل آخر من وسائل التقنية المتشابهة.[5]

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، (ص20).

[2] محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت (دراسة مقارنة)، ط1، دار لفكر والقانون للنشر والتوزيع، مصر، 2013، (ص8).

[3] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2008، (ص20).

[4] محمود أحمد طه، المرجع السابق، (ص8).

[5] خالد ممدوح إبراهيم،، المرجع السابق، (ص26).

4. **المجرم المعلوماتي:** وهو شخص يتمتع بالمهارة والمعرفة والوسيلة والسلطة وكذلك الباعث[1]، من أجل تنفيذ نشاطه الإجرامي.

فالجاني في جرائم التقنية شخص طبيعي، يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي، ولا نقصد هنا المستوى الرفيع العالي من المعرفة، فإن الجريمة وإن كانت ترتبط بتقنية نظم المعلومات والحاسب الآلي من حيث السعه والأسلوب والنتيجة، إلا أن الحد الأدنى من المعرفة يكفي لظهور الجريمة وإمكان ارتكابها خصوصا إذا ما اتسعت دائرة الإجرام فاستعان الفاعل ذاته بغيره ممن يساعده في إيقاع الجريمة وارتكابها.[2]

ويُقسم مجرمو المعلوماتية (Cyber Criminels) إلى مجموعة من الطوائف المختلفة، وهذا التصنيف كان قائماً على أساس أغراض الاعتداء، وقد وجد الباحثون صعوبة في إيجاد تصنيف منضبط لمجرمي هذه التقنية والسبب راجع إلى التغير السريع الحاصل في نطاق هذه الظاهرة المرتبطة أساساً بالتسارع الرهيب في ميدان الكمبيوتر والإنترنت.

ومن أفضل التصنيفات لمجرمي التقنية تقسيم المجرمين إلى ثلاث طوائف، هي:

أ- **المخترقون أو المتطفلون:** وهذه الفئة من المجرمين تنطلق من دوافع التحدي وإثبات الذات والمقدرة التقنية، ويتسمون كذلك بصغر السن، وكذلك لا تتوافر لديهم دوافع حاقدة أو تخريبية أو ربحية فهم يسعون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها.[3]

ب- **مجرمو الكمبيوتر المحترفون:** تتمتع هذه الطائفة بسعة الخبرة والإدراك للمهارات التقنية، كما تتميز بالتخطيط والتنظيم للأنشطة التي يرتكبها أفرادها فهم يسعون من وراء ذلك إلى تحقيق الربح المادي بطريقة غير مشروعة، ويتم عمل هذه المجموعة في إطار منظم ينطبق على أفعالهم وصف الجريمة المنظمة[4]، وتُعد هذه الطائفة الأخطر من بين مجرمي التقنية.

---

[1] الدافع أو الباعث أو الغرض أو الغاية: تعبيرات لها دلالة اصطلاحية في القانون الجنائي، وهنا الباعث يكون إما من أجل: السعي إلى تحقيق المكسب المالي أو الانتقام من رب العمل وإلحاق الضرر به، الرغبة في اختراق نظام الكمبيوتر والتفوق على تعقيد وسائل التقنية، دوافع سياسية أو اقتصادية أو دينية جلال محمد الزغبي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الأردن 2010، (ص21).

[2] أسامة احمد المناعسة وجلال محمد الزغبي، المرجع السابق، (ص71).

[3] محمود أحمد طه، المرجع السابق، ( ص14).

[4] طارق إبراهيم الدسوقي عطية، عولمة الجريمة (الشراكة العالمية في الممارسات الإجرامية)، دار الجامعة الجديدة، د.ط، الإسكندرية، 2010، (ص238).


E-ISSN:2958-9967 P-ISSN:2958-9959 المجلد: 01 ، العدد: 02، السنة: 2023

**ج- الحاقدون:** تسعى هذه الطائفة من المجرمين إلى الرغبة في الانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية عندما لا يكونوا موظفين فيها. ويغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات والبرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطياته.[1]

وتجدر الإشارة إلى أنه إزاء التصدي لظاهره الإجرام المعلوماتي لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، حيث ذهب جانب إلى تناولها بالتعريف على نحو ضيق، وجانب آخر عرفها على نحو متسع.

أما بالنسبة للمشرع الجزائري فلم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة، مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، مُعتبراً أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلاً للجريمة.

**أ – التعريف الضيق للجريمة الإلكترونية**

ما ذهب إليه الفقيه **MERWE** حيث يرى أن الجريمة المعلوماتية[2]هي: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات".[3]

ويرى الأستاذ **MASS** أن المقصود بالجريمة المعلوماتية: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح.[4]

كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديداً، ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة سمة الجريمة المعلوماتية.[5]

وجُل هذه التعريفات تعرضت للنقد من قبل الفقه، لذلك حاول جانب آخر من الفقه تعريف الجريمة الإلكترونية على نحو واسع من أجل محاولة تفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي.

---

[1] محمود أحمد طه، المرجع السابق، (ص15). وأيضا طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص237).

[2]مصطلح المعلوماتية: Informatique هي اختصار مزجي لكلمة معلومة Information وكلمة آلي: Automatique، وهي تعني المعالجة الآلية للمعلومة.

[3]طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص208).

[4]نهلا عبد القادر المومني، المرجع السابق، (ص48).

[5]محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001، (ص72).

**ب – التعريف الواسع لمفهوم الجريمة الإلكترونية**

من بين التعريفات الموسعة للجريمة المعلوماتية ما ذهب إليه من الفقه الأستاذ هلالي عبد الله أحمد بقوله: "عمل أو امتناع عن عمل يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للاعتداء عليها عقاباً.[1]

ويمتاز هذا التعريف بالمزايا التالية:

✓أنه يحتوي على كل صور الاعتداء الإيجابية أو السلبية التي توقع أضراراً بمكونات الحاسب المادية أو المعنوية.

✓أنه يتضمن الأثر الجنائي المترتب على العمل أو الامتناع غير المشروعين والذي يتمثل في الجزاء الجنائي بشتى صوره وأنواعه.

✓يحافظ على الشرعية الجنائية: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون".[2]

ونظراً لخطورة هذه الجريمة وآثارها الممتدة التي قد تصل من دولة لأخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات هيئة التعاون الاقتصادي للتنمية OECD، التي اتخذت التعريف التالي كتعريف لجريمة الكمبيوتر بأنها: "أي سلوك غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يُعتبر اعتداءً على الكمبيوتر".[3]

بعد التطرق إلى تعريف الجرائم الإلكترونية التي تعد إفرازاً ونتاجاً لتقنية المعلومات نخوض في البحث عن خصائص هذه الجريمة التي تميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجوعة من السمات، قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية.

**المطلب الثاني: خصائص الجريمة الإلكترونية**

يصعب متابعة جرائم الحاسب الآلي والإنترنت وكذا الكشف عنها، لأن هذه الجرائم لا تترك أثراً فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ومعظم جرائم الحاسب الآلي

---

[1] عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي(دراسة مقارنة)، دار النهضة العربية، القاهرة، 2000، (ص105).

[2] راجع المادة الأولى من الأمر (66/ 154) المؤرخ في 8 حزيران/ يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم.

[3] طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص214 و215).


E-ISSN:2958-9967 P-ISSN:2958-9959 المجلد: 01 ، العدد: 02، السنة: 2023

تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، وتعود أسباب صعوبة إثبات هذا النوع من الجرائم إلى الأمور الآتية:

- ✓ أنها كجريمة لا تترك أثراً بعد ارتكابها ويصعب الاحتفاظ بأثرها إن وجدت.[1]
- ✓ تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.
- ✓ أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها.

بالإضافة إلى أن ارتباط الجريمة الإلكترونية بجهاز الحاسب الآلي وشبكة الإنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية، ولعل من أهمها ما يلي:

- الخاصية الأولى: جرائم الحاسوب ترتكب بواسطة الحاسب الآلي وكذلك عبر شبكة الإنترنت فهي حلقة الوصل الرئيسية بين الأهداف المحتملة كافة لتلك الجرائم كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم.[2]
- الخاصية الثانية: أنها جريمة عابرة للحدود، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهذا خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى شكليات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.[3]
- الخاصية الثالثة: صعوبة التحري والتحقيق نظراً لارتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، فالتحري عنها ينطوي على العديد من المشكلات والتحديات الإدارية والقانونية، والتي تتصل ابتداء من عملية ملاحقة الجناة، فإذا تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة.[4]
- الخاصية الرابعة: تتسم بالخطورة البالغة من عدة جوانب، فمن ناحية أولى نجد الخسائر الناجمة عنها كبيرة جداً قياساً بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية نجدها ترتكب من فئات متعددة تجعل من التنبؤ بالمشيئة فيه أمراً صعباً، ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة.

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص222).

[2] أمير يوسف فرج، المرجع السابق، (ص16).

[3] فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011- 2012، (ص 43).

[4] محمود أحمد طه، المرجع السابق، (ص13).


المجلد: 01 ، العدد: 02، السنة: 2023 P-ISSN:2958-9959 E-ISSN:2958-9967

ولا أدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقاً لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية في نهاية القرن الماضي حولي 500 مليون دولار في السنة، وذلك في نهاية القرن العشرين.[1]

- الخاصية الخامسة: الصورة التقليدية للمجرم تكاد تختفي في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين ونادراً ما يكون محترفاً للإجرام أو عائداَ، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة، وذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية.[2]
- الخاصية السادسة: قلة الإبلاغ عن وقوع الجريمة المعلوماتية، وذلك راجع لسببين: أولهما الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الإنترنت تم الكشف عنها بالصدفة أو بعد فترة طويلة من ارتكابها، والسبب الثاني هو عدم اكتشاف الضحية للجريمة، ما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها.[3]

وعليه فالجريمة الإلكترونية تعتبر من أحدث أنواع الجرائم، مسرحها العالم الافتراضي غير ملموس بعيدة عن أي مظهر من مظاهر الجريمة التقليدية، فهي جريمة عابرة للحدود يرتكبها مجرمون ذوو مستوى عال، أذكياء ومتميزون في المجال التقني، ما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها والتحري عنها، أو الوصول إلى مرتكبها.

وقد صنف الفقهاء والدارسون جرائم الكمبيوتر والإنترنت ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، وهذا ما سنتعرض إليه فيما يلي:

## المطلب الثالث: تصنيف الجرائم الإلكترونية

يصعب تصنيف الجرائم نظراً لاختلافها من مجتمع لآخر من حيث تطوره، ومدى استخدامه للحاسوب ودرجة اعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع اتفاقية جرائم الكمبيوتر والإنترنت لعام 2001 (اتفاقية بودابست 2001) تضمن أربع طوائف رئيسية:

أ- الجرائم التي تستهدف سلامة وسرية المعطيات والنظم: وتضم الدخول غير قانوني (غير مصرح به)، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم.

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص287).

[2] سفيان سوير، جرائم للمعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، -2010-2011، (ص18 و19).

[3] خالد ممدوح إبراهيم، المرجع السابق، (ص19 و20).

ب- الجرائم المرتبطة بالكمبيوتر: تضم التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر.

ج- الجرائم المرتبطة بالمحتوى: وهي تضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.[1]

د- الجرائم المرتبطة بالأشخاص والأموال: وتضم السرقة والاحتيال والتزوير والاطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية، وإساءة استخدام المعلومات، القرصنة ... وغيرها من الجرائم.[2]

وعليه، فقد تعددت الجهود الفقهية التي بُذلت على الصعيد الدولي أو الوطني من أجل وضع تقسيم يمكن الاعتماد عليه لجرائم المعلوماتية، وفي هذا المجال يمكن تقسيمها إلى مجموعتين أساسيتين:

**المجموعة الأولى:الجرائم التي تقع على الإنترنت**

أي أن الشبكة العنكبوتية تكون عنصراً سلبياً في الجريمة أي محل للجريمة فقط، فإن هدف المجرم ينصب حول البيانات والمعلومات المخزنة والمنقولة عبر القنوات الخاصة أو العامة واختراق الحواجز الأمنية إن وجدت والاعتداء على الأموال، والتي نذكرها على التوالي.

**أ- سرقة المال المعلوماتي:**

أضحى لبرامج المعلومات قيمة غير تقليدية لاستخداماتها المتعددة في المجالات الاجتماعية والاقتصادية كافة، فهذه القيمة المميزة لبرامج المعلومات تجعلها محلاً للتداول، وهنا تبدو أهمية الإنترنت بصفته مصدر المعلوماتية، ما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة، عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين:

أن تكون المعلوماتية أداة أو وسيلة للاعتداء، وأن تكون المعلوماتية موضوعاً للاعتداء وسرقة تلك المعلومات.

---

[1] محمود أحمد طه، المرجع السابق، (ص18).

[2] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، ط1، دار البداية، عمان، 2012، (ص 134).

فالزاوية الأولى يستخدم الجاني المعلوماتية لتنفيذ جرائم سواء ما تعلق منها بجرائم للاعتداء على الأشخاص أو الأموال كالسرقة والنصب وخيانة الأمانة، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها.[1]

ب- **استخدام البروكسي للدخول إلى المواقع المحجوبة:** هو عبارة عن برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد، وهذا البرنامج يستخدم لتجاوز المواقع المحجوبة، والتي عادة ما تكون إما مواقع جنسية أو سياسية معادية للدولة.[2]

ج – **جرائم الاختراق:** يمثل الاختراق المعلوماتي تحدياً على قدر كبير من الأهمية لإنجازات تكنولوجيا المعلومات، ويعرفه شراح القانون المعاصرون بأنه: "فعل مشروع يوظف المعرفة العلمية السائدة في ميدان ثقافة الحاسوب والمعلوماتية لاقتراف إساءة أو هجوم على الغير".[3]

فهي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، يقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات للأغراض الشرعية مثل اللعب بالحسابات الشخصية ومزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف.[4]

وفيها تعرض بعض الأساليب المستخدمة في عمليات الاختراق:

1. الاقتحام أو التسلسل.
2. الفيروسات.

د – **المواقع المعادية:** بعض المواقع يتم إنشاؤها لمعاداة سياسية أو معاداة الدين أو الأشخاص أو الجهات.

هـ – **جرائم القرصنة:** تواجه شبكة الإنترنت ما يسمى بظاهرة القرصنة، والتي تكون من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تحترق أجهزة الحاسوب، وكذا الأرقام السرية للأشخاص وإلى بريدهم الإلكتروني.

---

[1] منال هلال المزاهرة، تكنولوجيا الاتصال والمعلومات، دار السيرة، الأردن، 2014، (ص376).

[2] محمد عبد الله منشاوي، المرجع السابق، (ص32).

[3] مصطفى عثمان ضياء، المرجع السابق، (ص40).

[4] علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، الأردن، 2007، (ص432).

فهي تعتبر سرقة للخدمات أو الاستعمال غير المصرح به للنظام المعلوماتي.[1]

و – **جرائم التجسس الإلكتروني:** هي الجرائم التي يتم بواسطتها اختراق أجهزة المستخدمين بطرق غير شرعية ولأغراض غير سوية، من أجل سرقة معلومات تتعلق بذلك المستخدم سواء على الصعيد الشخصي، أو السياسي أو العلمي أو الاجتماعي، حيث لم يُعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو "الهاكرز".

فهي ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا.[2]

ز – **الإرهاب الإلكتروني:** يُعد الإرهاب المعلوماتي من أخطر أصناف الجرائم المرتبطة بتكنولوجيا المعلوماتية نظراً لأثرها ودوافعها، فالإرهاب الإلكتروني هو تحطيم أو إتلاف أنظمة معلوماتية بهدف المساس، أو إحداث خلل يمس باستقرار دولة أو بهدف الضغط على حكومة ما.[3]

فهو هجوم مع سبق الإصرار، ذو أهداف سياسية ضد المعلوماتية، ضد أهداف مسلحة (الشرطة، الدرك أو أهداف عسكرية)، أو غير مسلحة (كالإدارات المدنية الوطنية)، من طرف جماعات وطنية أو خفية.[4]

وتزداد خطورة الإرهاب الإلكتروني في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، ما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الجوية وشل أنظمة القيادة.

**المجموعة الثانية: جرائم تقع بواسطة الإنترنت**

أي أن الشبكة دورها إيجابي في ارتكاب الجريمة، فهي تسهل للمجرم المعلوماتي تحقيق غايته، ويلاحظ أن أغلب صورها في هذه الحالة تشكل الجرائم الواقعة على الأشخاص.

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، (ص248).

[2] اطلع على الموقع الإلكتروني WWW.abahe.co.uk>71102-piracy: تاريخ الإطلاع: 2019/03/13، ساعة الإطلاع: 19:45.

[3] نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري، مذكرة ماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012- 2013، (ص155).

[4] Sophie Revol, (DESS) Droit du Multimédia et de l'informatique, « Terroriste et Internet », sous la direction de N.KOSTIC , Université Paris II Pantheon Assas année 2002-2003(France), page.9

1. الجرائم الجنسية والممارسات غير الأخلاقية.
2. الجرائم المالية: والتي تضم كلاً من:

أ. **جرائم السطو على أرقام البطاقات الائتمانية:** والتي يتم ارتكابها باستخدام تكنولوجيا المعلومات، سرقة الأقراص الصلبة والمرنة، بغرض الحصول على المعلومات التي تحويها ويتولى قراصنة المعلومات بيعها بعد الحصول عليها، نظير الحصول على عائد مادي، مثال ذلك: الوصول إلى أجهزة الحاسب الخاصة بمكاتب الائتمان الرئيسية وسرقة المعلومات الائتمانية، تم استخدامها بإعادة بيعها لأشخاص آخرين، وتدمير المشروعات المهمة للشركات بغرض ابتزازهم.[1]

ب. **القمار عبر الإنترنت:** مع الانتشار الواسع والتطور الكبير لشبكة الإنترنت على مستوى العالم ظهر إلى الوجود. صفحات القمار تتمثل في الكازينوهات الافتراضية، وهي عبارة عن مواقع ويب تم تصميمها على طراز كازينوهات "لاس فيغاس" الأمريكية، وتتوفر كل أنواع القمار وألعابه ابتداءً من ألعاب الورق، وانتهاء بآلات المقامرة، وهي موجودة على شبكة المعلوماتية.

ج. **تزوير البيانات:** لا تكاد تخلو جريمة من عملية تزوير للبيانات بشكل أو بآخر، ويتم تزوير بيانات الحاسب إما بإدخال بيانات مغلوطة إلى الموظفين المسموح لهم بإدخال البيانات، ثبت أنه كان لهم ضلع كبير في الكثير من جرائم نظم المعلومات.[2]

د. **الجرائم المنظمة:** هي عنف منظم قصد الحصول على مكاسب مالية، بطرق وأساليب غير مشروعة، وتمارس الجريمة على شكل نصب واحتيال وتزوير وسطو وخطف من أجل الابتزاز والقتل.....الخ، إلا أنها تختلف عن الجرائم المعروفة كونها تنفذ عن بعد تدبير وتنظيم، لذا سميت بـ "الجريمة المنظمة".[3]

**المبحث الثاني: ثبات النص الجزائريوموائمته مع الاتفاق الدولي لمواجهة الجريمة المعلوماتية**

لقد أثبت الواقع العملي أنه لا يمكن لدولة وحدها مكافحة الجريمة المعلوماتية وكسر شوكة تفشي هذه الظاهرة المستحدثة كيف ما كانت الإمكانيات التي تتوفر عليها في هذا الإطار.

حيث أنه ليس من المهم التوفر على ترسانة تشريعية وقضائية وفنية في مجال مكافحة جريمة المعلوماتية، بل أن تكون هذه القوانين متجانسة وملائمة مع قوانين مختلف الدول هذا من جهة، وملائمة

---

[1] فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة، ط1، دار الهومة للطباعة والنشر والتوزيع، الجزائر، 2014، (ص247).

[2] منال هلال المزاهرة، المرجع السابق، (ص40 و41).

[3] يشير مصطلح الجريمة المنظمة: إلى جماعات ترتكب أفعالاً تخترق بها القانون للحصول على مساعدات مادية، كما تهتم بالابتزاز والخدع، والإنتاج والتوزيع غير القانوني لإدمان المخدرات، والتعامل مع السلع الممنوعة مثل الأسلحة غير القانونية، فهي تمتاز بخاصيتين: التنظيم، والكسب المادي. راجع: نصرة تامي، الإعلام القضائي والإرهاب، ط1، دار أسامة للنشر والتوزيع، الأردن، 2015، (ص87).

قوانين هذه الدول مع نصوص الاتفاقية التي صادقوا عليها من جهة أخرى؛ وذلك بهدف خلق منظومة قانونية موحدة بين دول تهدف إلى حماية المصلحة المشتركة.

## المطلب الأول: سعي المشرع الجزائري للتصدي للجريمة الإلكترونية

سعياً من المشرع الجزائري للتصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام والإتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية.

### أولا: أركان الجريمة الإلكترونية

تشترك أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن المادي والمعنوي وكذا الركن الشرعي.

- الركن المادي:

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علماً أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها.

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب مثلاً: جريمة التجسس الإلكتروني، الركن المادي فيها هو: الحصول مباشرة على الدعامة الإلكترونية الحاوية لهذا السر أو المعلومات، كالحصول على قرص مدمج "CD" مخزنة فيه الأسرار والوثائق.[1]

- الركن المعنوي:

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين: العلم والإرادة.

- العلم: هو إدراك الفاعل للأمور.
- الإرادة: فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

وطبقاً للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاماً وخاصاً. وعليه فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء، ولكن هذا لا يمنع من أن بعض الجرائم الإلكترونية يتوافر فيها القصد الجنائي الخاص (مثلاً: جرائم تشويه السمعة عبر الإنترنت)، وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.

---

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، (ص49 و50).

**ثانياً: القوانين المتعلقة بالجريمة الإلكترونية**

لقد خصَّ المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة، وهذا ما سنتطرق إليه لاحقاً.

**أ. قانون العقوبات:**

لقد تعرض المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي في قانون العقوبات بموجب القانون (15/04)[1]، تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، ويتضمن هذا القسم ثماني مواد من المادة (394) مكرر إلى (394 مكرر 8).

وفي عام 2006، أدرج المشرع تعديلاً آخر على قانون العقوبات بموجب القانون (23/06)[2]، حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

ويرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى.

أما بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في قانون العقوبات، يمكن تصنيفها إلى ما يلي:

1. الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
2. حذف أو تغيير لمعطيات المنظمة.
3. إدخال أو تعديل في نظام المعطيات.
4. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار.
5. حيازة أو إفشاء أو نشر أو استعمال المعطيات.
6. تكوين جمعية الأشرار.

وعليه، يمكن تكييف هذه الأفعال الإجرامية بأنها جرائم ضد أموال الغير والمضرة بالمجتمع.

[1] القانون رقم (15/04) المؤرخ في 10 تشرين الثاني/ نوفمبر 2004 المعدل والمتمم لقانون العقوبات، (جريدة رسمية عدد71).

[2] القانون رقم (23/06) المؤرخ في 20 كانون الأول/ ديسمبر 2006 المعدل والمتمم لقانون العقوبات ،(جريدة رسمية عدد84).

وتجدر الإشارة إلى أن المشرع قد قام بتعديل قانون العقوبات في سنة 2016، مستحدثاً بذلك نصاً جديداً وهو المادة (87 مكرر 12) والتي أحدثت لنا جريمة جديدة وهي جناية تجنيد الأشخاص لصالح غرابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال.[1]

**ب. قانون الإجراءات الجزائية:**

فيما يتعلق بمتابعة الجريمة الإلكترونية فهي تتم بالإجراءات نفسها التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة، واستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية.[2]

كما نص على التفتيش في المادة (45 الفقرة 7) من القانون نفسه[3] المعدلة، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة من حيث الشروط الشكلية والموضوعية.

ونص كذلك المشرع على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة (51 الفقرة 6) وكذلك على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

أما بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنه تطبق عليه إجراءات الجريمة التقليدية نفسها.

**ج. القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:**

يهدف هذا القانون[4]، إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

---

[1] القانون رقم (02/16) المؤرخ في 19 أيار/ مايو 2016 المعدل والمتمم لقانون العقوبات، (جريدة رسمية عدد37).

[2] انظر المادة (37) من القانون رقم (07/17) المؤرخ في 27 آذار/ مارس 2017 المعدل والمتمم لقانون الإجرات الجزائية، (جريدة رسمية عدد 20).

[3] المادة (45) الفقرة الثانية من نفس القانون نفسه (07/17) سالف الذكر.

[4] القانون رقم (04/09) المؤرخ في 05 آب/ أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، (جريدة رسمية عدد 47).

وقد تبنى هذا القانون تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكل ما يتعلق بالمنظومة المعلوماتية، وكذا معطيات المعلومات ومقدمو الخدمات.[1]

وقد خول هذا القانون بعض الإجراءات التي تطبق على الجرائم الإلكترونية من:

- مراقبة الاتصالات الإلكترونية.
- تفتيش المنظومة المعلوماتية.
- حجز المعطيات المعلوماتية.

وقد أنشئت بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتي من مهامها:

- تفعيل التعاون القضائي والأمني وإدارة وتنسيق العمليات الوقائية.
- تبادل المدعومات مع الجهات الأجنبية من أجل تفعيل الحماية على المنظومة المعلوماتية من كل خطر يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[2].

**المطلب الثاني: التصدي الدولي للإجرام المعلوماتي**

**اتفاقية الجرائم الإلكترونية- مجلس أوروبا[3] (The Convention on Cybercrime– Council of Europe)** التي اعتمدتها لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة المنعقدة بتاريخ الثامن من كانون الأول/ ديسمبر 2001، والمعروفة باتفاقية بودابست؛ المدينة التي فُتح فيها باب التوقيع على الاتفاقية بتاريخ الثالث والعشرين من الشهر والسنة نفسهما، وذلك لمناسبة انعقاد المؤتمر الدولي حول الجريمة الإلكترونية.

ولم تقتصر هذه الاتفاقية على الدول الأعضاء في مجلس أوروبا بل إنها قد سمحت بمقتضيات مادتها السادسة والثلاثين بالتوقيع عليها، حتى قبل دخولها حيز التنفيذ، من دول من خارج المجلس وهو ما

---

[1]راجع المادة (2) من القانون رقم (04/09) المؤرخ في 05 آب/ أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[2]راجع المادة (04، 05، 06) والمادتين (13، 14) من القانون رقم (04/09) المؤرخ في 05 آب/ أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[3]مجلس أوروبا هو منظمة دولية تأسست في عام 1949، ويتكون من 47 دولة أوروبية، يقع مقر للمجلس في مدينة ستراسبورغ الفرنسية وعضويته مفتوحة لكل دول أوروبا الديمقراطية، وهو ليس جزءاً من الاتحاد الأوروبي ويختلف عن مجلس الاتحاد الأوروبي والمجلس الأوروبي. مع العلم أن الجزائر لم تصادق على هذه الاتفاقية. وإنما أخذت بعض قواعدها وأدرجتها في منظوماتها القانونية الداخلية.

حصل بالفعل مع كل من: كندا واليابان وجنوب افريقيا والولايات المتحدة الامريكية،[1] ليستمر بعد ذلك الانضمام إلى هذه الاتفاقية من قِبل المزيد من الدول، بما جعل منها آلية دولية لمكافحة الإجرام المرتكب بوسائل تقنيات المعلوماتية وضدَّها.

وقد نظمت الوزارة المكلفة بتقنيات الإعلام والاتصال بالتعاون مع خبراء دوليين في هذا المجال ورشة تحت عنوان: إعداد مسار انضمام موريتانيا إلى اتفاقية بودابست حول الجريمة الشيبانية، للفترة من 17 إلى 19 كانون الثاني/ يناير 2018، وهو ما يمكن اعتباره خطوة في طريق الانضمام الفعلي لهذه الاتفاقية.[2]

وتستفيد الدول التي تنضم إلى الاتفاقية من الخبرات والإمكانات التي تتمتع بها الدول الأعضاء المتقدمة تكنولوجياً كالدول الأوروبية والولايات المتحدة الأمريكية واليابان، كما تستفيد كذلك من تعاون الفاعلين الأساسيين في مجال تقنية المعلومات والاتصال كـ: **Facebook**, **Google**, **Gmail**, **Youtube** وذلك في التحريات والتصدي للجريمة كسحب فيديو من اليوتيوب مثلاً، أو الحصول على معلومات من شأنها المساعدة في التعرف على هوية صاحب حساب في Yahoo متورط في ارتكاب جريمة، أو توقيف حساب على الفيسبوك ينشر محتوىً مجرماً بالنصوص الوطنية أو الدولية.[3]

ولأن هذه الاتفاقية قد جاءت سابقة على الكثير من القوانين الوطنية والاتفاقيات الإقليمية، فإن شكلها من حيث البنية النصية، ومضمونها من حيث وضع معانٍ للمصطلحات المستخدمة في هذا المجال وتعداد الأفعال المجرّمَة سواء منها ما تعلق بالاعتداء على شبكة تقنية المعلوماتية نفسها، أو ما استخدمت له هذه التقنية من أغراض الاعتداء على حقوق الأفراد وثقافة المجتمعات وأمن الدول، وكذلك وضع القواعد الإجرائية وأسس التعاون الدولي في مجال مكافحة هذه الجريمة، كل ذلك قد عكسته النصوص اللاحقة على نفاذها، وذلك على النحو الذي سبق التطرق إليه في معرض تناول التدابير التشريعية في مجال محاربة الجريمة الشيبانية على الصعيد الوطني والإقليمي.

من كل ما تقدم نخلص إلى أن الثورة الرقمية، التي غيرت الشكل التقليدي للمجتمعات، وجعلت من سوق تقنيات الاتصال؛ من حواسيب وهواتف وألواح إلكترونية وغيرها، السوقَ الأكثر رواجًا، وعلى الرغم

[1] التقرير التفسيري لاتفاقية الجريمة الإلكترونية https://rm.coe.int/explanatory-report...convention-in

[2] www.ami.mr/Depeche-56093.html

[3] http://www.mf-ctrf.gov.dz/presse/Bulletin%2032%20Cyber.pdf

مما حملت معها من مزايا على صُعُد الحياة المختلفة، فإنها لم تسلم من سوء الاستعمال والاستغلال في ارتكاب جرائم تطال الفرد والمجتمع والدولة.

لقد تجاوز تطور تكنولوجيا المعلوماتية من خلال شبكة الاتصال فائقة السرعة، المفاهيم القانونية السائدة لاسيما بالنسبة للقانون الجنائي الذي تم وضعه للتعامل مع واقع مادي لا افتراضي وليطبق في نطاق حدود الدولة الواحدة لا على الصعيد العالمي.

لقد مثلت ضرورة تحديث وتطوير ومواءمة قواعد القانون الجنائي؛ الموضوعي منها والشكلي، مع هذا الواقع الجديد تحديًا، وإنْ اختلفت الدول في الترتيبات الفنية للتعامل معه، فقد اتحدت في الوعي بضرورة مواجهته.

**المطلب الثالث: الجهود الإقليمية لمجابهة الإجرام المعلوماتي**

لأن الجريمة الشيبانية عابرة للحدود غير مكترثةٍ بالحواجز الطبيعية أو الثقافية، ومن شواهد ذلك الكثيرة انتشار فيروسات الحاسوب بسرعة وعلى نطاق واسع، ولأن مرتكبيها غالباً ما يكونوا متواجدين في أماكن غير تلك التي تُنتِج فيها الجريمة آثارها، فقد اقتضى الأمر من دول العالم التنسيق والتعاون في مجال محاربتها ووضع التصورات المشتركة بشأنها، وذلك من خلال أطر التعاون والتكتل الإقليمي وكذلك على الصعيد الدولي، وفي هذا السياق جاء اتفاق الدول العربية على وضع آلية تعاون خاصة بها تتمثل في:

**أولا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:** الموقعة بتاريخ 21 كانون الأول/ ديسمبر 2010، والتي تهدف بحسب مقتضيات مادتها الأولى إلى تعزيز التعاون بين الدول الأعضاء في مجال مكافحة جرائم تقنية المعلومات بما تمثله من خطر على أمن ومصالح الدول والمجتمعات والأفراد.[1]

ويتضح من خلال بنية نص الاتفاقية ومضمون الترتيبات التي قضت بها أنها ألهمت النصوص العربية اللاحقة على توقيعها وقد جاء ذلك صريحاً في بعض هذه النصوص، من ذلك ما جاء في المذكرة الإيضاحية لقانون مكافحة جرائم تقنية المعلومات الكويتي، والذي أخذ بالتسمية نفسها التي أعطتها الاتفاقية لهذه الجرائم، من أن إعداد هذا القانون يأتي التزامًا(بأحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها دولة الكويت بموجب القانون رقم (60 لسنة 2013).[2]

---

[1] المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المذكرة الإيضاحية للقانون الكويتي رقم (63) لسنة 2015، المتعلق بمكافحة جرائم تقنية المعلومات.

وقد حددت الاتفاقية مجال تطبيقها في أربع نقاط وردت على النحو الآتي:

- . إذا ارتكبت إحدى هذه الجرائم في أكثر من دولة.
- . إذا كانت الجريمة المرتكبة في الدولة العضو قد تم التخطيط والإعداد لها أو الإشراف والتوجيه بشأنها، في دولة أو دول أخرى.
- . إذا كانت الجهة الضالعة في ارتكاب الجريمة، جماعة إجرامية منظمة، لها أنشطة في أكثر من دولة.
- . إذا كان للجريمة المرتكبة في إحدى الدول آثاراً بالغة الخطورة والضرر على دولة أو دول أخرى.[1]

وعلى الرغم من تأكيد الاتفاقية على احترام سيادة الدول الأعضاء، لاسيما في مجال الولاية القضائية وغيرها من وظائف السيادة، فإنها ألزمت كل دولة في نطاق احترام تشريعاتها وأنظمتها الداخلية، بتجريم الدخول والبقاء غير المشروعين إلى تقنية المعلومات أو اعتراض سير بياناتها وإساءة استخدام وسائلها والاحتيال بواسطتها وكذا الاعتداء على الحياة الخاصة والملكية الفكرية والجرائم المتعلقة بالإرهاب والمواد الإباحية وبالاستخدام غير المشروع لأدوات الدفع الالكترونية[2]، كما ألزمت الاتفاقية في مادتها الحادية والعشرين، الدول الأطراف بتشديد العقوبات المقررة للجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

ولأن الأمر يتعلق باتفاقية بين عدة دول فقد تم تكريس فصل كامل للتعاون القانوني والقضائي شمل مسائل الاختصاص وتسليم المجرمين والمساعدة المتبادلة، مع التوصية بإنشاء جهاز خاص بطاقم بشري مؤهل من اجل ضمان حسن سير هذا التعاون.[3]

وعلى غرار الدول العربية وفي سياق الوعي المتنامي بخطورة الجريمة الشيبانية وضرورة مواجهتها بالوسائل التشريعية، الفنية والمؤسسية للازمة، نحت الدول الإفريقية المنحى نفسه وذلك من خلال:

**ثانيا: اتفاقية الاتحاد الإفريقي حول الأمن الشيباني وحماية البيانات ذات الطابع الشخصي:** وقد تم تبنيها من قِبل دول الاتحاد الإفريقي لمناسبة انعقاد مؤتمره الثالث والعشرين في دورة عادية، بتاريخ 27 حزيران/ يونيو 2014، بمدينة مالابو عاصمة جمهورية غينيا الاستوائية.

---

[1] المادة (03) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المواد من (05 إلى 18) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] المواد من (30 إلى 43) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

نُظمت هذه الاتفاقية بنصٍ واحدٍ من ثمانٍ وثلاثين مادة، أربعة مجالات تناولها المشرع الموريتاني بنصوص منفصلة على النحو الذي تقدم، وهذه المجالات هي:

- الجريمة الشيبانية بأبعادها المختلفة الموضوعية والإجرائية.
- حماية البيانات ذات الطابع الشخصي.
- تنظيم المبادلات الإلكترونية.
- رسم أهداف ووضع ضوابط لتنظيم وترقية مجتمع المعلوماتية في دول الاتحاد.

ونرى أن إفراد مشرعنا لكل من هذه الميادين الأربعة بنص، مسلك موفق لا يحول دون تكامليتها من حيث الأهداف والتنظيم.

وعلى الصعيد شبه الإقليمي تبنت المجموعة الاقتصادية لدول غرب إفريقيا المعروفة اختصارًا بـ (CEDEAO) في الدورة السادسة والستين لمجلس وزرائها المنعقد في أبوجا أيام (17،18 و19) آب/ أغسطس 2011، اتفاقية لمحاربة الجريمة الشيبانية في فضاء المجموعة اشتملت تقريباً على محاور ومضمون النصوص الوطنية نفسها، الإقليمية والدولية في هذا المجال.[1]

**الخاتمة:**

جالت بنا هذه الأوراق البحثية إلى التعريج بأن العالم يعيش اليوم ثورة ثالثة، أو الموجة الثالثة كما يسميها البعض وهي ثورة تكنولوجيا المعلومات والمعرفة، والتي أصبحت أساساً للتنمية وزيادة الإنتاج، وسرعة اتخاد القرار الصحيح، وقد تمخض عن هذا التطور انتشار ما يعرف بالجريمة الإلكترونية والتي تتمتع بطبيعة قانونية خاصة تميزها عن الجريمة التقليدية.

ومن المؤكد أن المشرع على غرار نظرائه وضع ترسانة قانونية جزائرية في مجال مكافحة الجرائم المعلوماتية، واتضح أن قانون العقوبات تضمن فصولاً تشكل الأداة الأساسية لمكافحة هذا النمط الجديد من الإجرام –في محاولة منه للتصدي لهذا النوع من الجرائم ومكافحتها بشتى الطرق–، كما أن هناك مجموعة من المقتضيات الزجرية المتفرقة في المعاهدات الإقليمية والدولية–التي صادقت الجزائر عليها– ذات علاقة بالمجال المعلوماتي، والتي تكمل تلك الموجودة بالمجموعة الجنائية الجزائرية.

[1]Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

كما لوحظ بأن المشرع الجزائري خطا منهج خطوات إيجابية في مجال سن تشريعات حديثة لمواجهة الجريمة المعلوماتية، وبالتالي أصبح للقاضي الجزائي آليات البت في قضايا الجريمة الإلكترونية، خصوصاً القضايا المتعلقة بالمعطيات الشخصية والمساس بها.

## قائمة المصادر والمراجع:

### أولاً: الكتب والمؤلفات


1. جلال محمد الزغبي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2010.
2. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008.
3. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت (دراسة مقارنة)، ط1، دار الفكر والقانون للنشر والتوزيع، مصر، 2013.
4. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2008.
5. جلال محمد الزغبي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2010.
6. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008.
7. طارق إبراهيم الدسوقي عطية، عولمة الجريمة (الشراكة العالمية في الممارسات الإجرامية)، دار الجامعة الجديدة، د.ط، الإسكندرية، 2010.
8. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001.
9. عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2000.
10. فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة، ط1، دار الهومة للطباعة والنشر والتوزيع، الجزائر، 2014.
11. نصرة تامي، الإعلام القضائي والإرهاب، ط1، دار أسامة للنشر والتوزيع، الأردن، 2015.
12. علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، الأردن، 2007.
13. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، ط1، دار البداية، عمان، 2012.
14. منال هلال المزاهرة، تكنولوجيا للإتصال والمعلومات، دار السيرة، الأردن، 2014.
15. Sophie Revol, (DESS) Droit du Multimédia et de l'informatique, « Terroriste et Internet», sous la direction de N.KOSTIC , Université Paris II Pantheon Assas année 2002-2003(France).


### ثانياً: الرسائل والأطروحات العلمية


1. درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسة، جامعة تلمسان، 2016-2017.
2. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسة، جامعة باتنة، 2013.
3. وأيضا: يوسف صعيدي، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسة، جامعة مولود معمري، تيزي وزو، 2013.
4. فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011- 2012.

5. سفيان سوير، جرائم للمعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010- 2011.

**ثالثاً: أهم النصوص القانونية**

1. القانون (رقم 04/09) المؤرخ في 05 آب/ أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، (جريدة رسمية عدد 47).
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات متوفرة على الرابط التالي:
https://www.courts.gov.ps/userfiles/file/%D8%A7%D9%84%D8%A7%D8%AA%D981%D8%A7%D9%82%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf
3. مجلس أوروبا: هو منظمة دولية تأسست في عام 1949، ويتكون من 47 دولة أوروبية، يقع مقر للمجلس في مدينة ستراسبورغ الفرنسية، وعضويته مفتوحة لكل دول أوروبا الديمقراطية وهو ليس جزءاً من الاتحاد الأوروبي ويختلف عن مجلس الاتحاد الأوروبي والمجلس الأوروبي.
http://www.mf-ctrf.gov.dz/presse/Bulletin%2032%20Cyber.pdf